WHAT IS CLAIMED IS:

1. A method for the distributed collecting of network data traffic statistics, wherein said network comprises end systems (ES) connected to network segments, comprising:

compiling individual networks performance statistics at a plurality of said ESs, said performance statistics based on data seen at said ESs;

transmitting data containing said statistics to a collector from a plurality of said ES;

compiling said statistics from individual ES into group network statistics; and

providing reports based on said compiled statistics, from said collector, to a network manager.

2. The method according to claim 1 further comprising:

transmitting data containing compiled statistics from said collector to a domain collector;

compiling statistics from a plurality of collectors at said domain collector;

providing reports based on said compiled statistics, from said domain collector, to a network manager.

3. The method according to claim 1 further comprising:

including in ESs participating in said distributing collecting an agent, said agent being an executable module invisible to a user for collecting traffic statistics.

4. The method according to claim 1 wherein said statistics collected are as defined in a stadard defined for the gathering of network-wide performance statistics.

5. The method according to claim 4 wherein said statistics collected are as defined by an RMON or RMON2 monitoring protocol.

6. The method according to claim 5 wherein said statistics collected are as defined by an RMON or RMON2 monitoring protocols published by in IETF RFC documents, RFC-1271, RFC-1513 and RFC-1757 and revisions.

7. The method according to claim 1 wherein said collector simulates the behavior of a standalone probe such that said manager interacts with and configures said collector as though said collector was a standalone probe and said collector configures said ESs.

8. The method according to claim 1 wherein said end systems communicate with a plurality of routers using protocols in a TCP/IP protocol suite.

9. The method according to claim 1 wherein a plurality of said ESs communicate using an ethernet protocol.

10. A bridge for use in a local area network comprising:

a plurality of ports capable of transmitting and receiving data on a network segment;

a plurality of shared buffer memories for buffering data received on said ports or waiting to be transmitted on said ports;

a bridge controller capable of reading the source and destination addresses of a data packet received on one of said ports; and

a collector for collecting data traffic statistics from agents operating on other devices in the network and a proxy for receiving configuration packets from a manager and communicating configuration data to said agents.

11. The apparatus according to claim 10 wherein said bridge collector forwards traffic statistics to a domain proxy.

12. The apparatus according to claim 10 further comprising a means for generating at said collector traffic statistics for multicast packets.

13. A local area network comprising:

a plurality of end systems, each with a connection to a network segment wherein said end systems are capable of transmitting data on said segment and werein at least one of sai end systems includes an agent for collection of traffic statistics; and

a plurality of collectors having connections to receive data from at least one agent in said ESs or from at least one other collector.

14. The local area network according to claim 13 wherein said collectors are further capable of detecting multicast packets and compiling traffic statistics on said packets.

15. The local area network according to claim 13 wherein said collectors are further capable of receiving probe configuration packets from a network manager and then sending configuration packets to each individual agent in the network.

Sub B7

16. A method for distributed remote network monitor (dRMON) in a LAN comprising:

deploying dRMON agents within ESs said agents implementing prior art RMON functional groups but only capturing and analyzing packets that their native ES sends or receives;

on a regular, periodic basis having the dRMON agents forward statistics and/or captured packets to a dRMON proxy or collector, existing somewhere on the WAN/LAN; and

combining received agent data thereby creating at the proxy the view that a prior-art stand-alone RMON probe would have if all the ES were on the same LAN segment with it.

17. The method according to claim 16 wherein said proxy can mimic the SNMP responses of a prior art non-distributed RMON probe so that existing network application management software can interact with the proxy as though the proxy were a prior art probe.

18. The method according to claim 16 wherein in a default mode, ESs in the same multicast domain are treated by a proxy as though they are on one LAN segment to RMON applications to interact with the proxy as though it were a prior art probe and in an enhanced dRMON Managers a user is provided with the ability to combine ports and hosts in order to create Virtual LAN (VLAN) definitions to cause the monitoring function to behave as though all selected hosts were on the same LAN segment being served by the same RMON probe with the dRMON collector in this embodiment creating and maintaining several such views with each appearing as one interface to conventional RMON Management applications.

Sub B7

19. The method according to claim 16 whereby said agents perform continual response time monitoring and forward the results to the Proxy.

20. The method according to claim 16 whereby said agemt software utilizes native OS APIs to gather information about the ES that could not be via packet capture and analysis, such as: (1) Network protocol stack configurations and NIC configurations including problematic situations; (2) Application information ranging from what protocols an application is bound to, to its manufacturer, version, file date and time, DLLs used and their versions, etc.; (3) System information such as memory, CPU, disk space, current resource utilizations, etc.; and (4) System performance metrics.

21. An agent for distributed network monitoring comprising:

an RMON Engine for receiving a packet stream coming from a DTA and subjecting it to RMON analyses as configured via the proxy;

RMON Data Structures;

filters;

an event generator;

Down-Loadable-Modules manager;

dRMON Interface Module; and

a protocol interface layer.

22. The agent of claim 21 implemented in the C programming language with executable code launched each time ES is started or rebooted and the agent may be tightly bound to ES adaptor driver software. Because the dRMON agent has no visible ES user interface, the ES user is totally unaware of the agents presence.

23. A proxy for distributed network monitoring comprising:

an agent discovery engine for automatically discovering all of the dRMON Agents within its management sphere;

a time-stamper for stamping statistics and packets received from agents;

an agent configuration for setting how much memory/storage to reserve for RMON data space, version management, etc.;

an RMON configuration for setting filters, historical sampling intervals and other MIB-defined user-settable options; and

an updater for automatically updating agents via the network.

add A6